



The Willows School

Information Security and Data Protection Policy

Ratified Date: September 2022

Review Date: September 2023

Background

As part of RMBC, The Willows School and staff are bound by the overarching RMBC Information Security Policy. All staff can access this via the HR portal. In addition, The Willows has a school-specific Information Security Policy, updated at least annually. The HR Portal will be checked at least annually for newer versions of the RMBC Policy.

Why protect information?

The Willows School holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this data could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal data could result in adverse media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Key Points of this Policy

- Do not leave confidential information lying around in school or at home.
- Do not leave members of the public unattended in rooms with confidential papers available.
- Do not let members of the public read confidential information on computer screens.
- Ensure confidential information and mobile computing equipment is transported securely in sealed bags and not left in cars.
- Ensure that all confidential information stored on laptops, hard drives, Google drive and USB pens is in encrypted files.

Information Security Policy Purpose

It is the policy of The Willows School to ensure that:

- Confidential information is protected from unauthorised access or disclosure.
- Information is accessible and available.
- Integrity of information is maintained.
- Information held by the school is protected from all threats, whether internal, external, deliberate or accidental.
- Regulatory and legislative requirements are met.
- All staff, Governors and partner organisations provided with authorised access to the school's equipment, are aware of information security issues and good practice.
- All breaches of information security, actual or suspected are reported, investigated, reviewed and acted upon.
- The SIRO (Senior Information Risk Owner) Committee has formulated an Acceptable User Policy (AUP).

Review

- The policy will be subject to an Annual Review by the SIRO Committee and will be amended as appropriate in response to changing organisational, legislative, environmental and technical requirements.

Scope

The Information Security Policy shall apply to all The Willows School staff, Governors, visitors and agents employed by the school and partner organisations provided with authorised access to the school's equipment systems, information and paper records.

Responsibilities of All Users

Applies to all permanent and temporary employees, Governors, contractors, agents, consultants, visitors and partner organisations with authorised access to Council equipment systems, information and paper records

It is the responsibility of each user to:

- Comply with this policy at all times.
- Comply with the Data Protection and Electronic Communications directives within the E-Safety Policy and AUP Policy.
- Request additional training if they are unclear about any aspect of this policy.

Physical Security

- Use the security measures we have in place such as electronic door controls, keypads, etc. Always challenge strangers.
- Visitors must sign in at reception and be escorted where necessary while on the premises. Extra care must be taken in areas where confidential information is stored and/or processed.
- A tidy and secure environment must be maintained and information must be stored appropriately.
- Members of the public must not be able to see computer displays where data or confidential information is likely to be shown.

Personal computers and workstations must be powered off at the end of each day, unless otherwise instructed.

Use of Equipment and Information:

- You must never attempt to sign on to any system using someone else's user ID.
- Documents containing personal, confidential or sensitive information must be disposed of by sending to the office for shredding. Homeworkers must ensure that confidential waste is returned to the school office to be destroyed.
- Unattended administration computer terminals or standalone computers and laptops used for administration must be turned off or password protected. (Curriculum Network computers log-out automatically).
- All employees should bear in mind that the loss or misuse of personal data can be judged an offence under the Data Protection Act.

Use of Mobile Computer Equipment and Homeworking/Travelling

- Staff must be aware of, and comply with, the school's directives on Data Protection, information security and use of electronic communications.
- Staff must only remove files and equipment from the workplace where there is a business need to do so, approved by SLT, and should be returned as soon as possible.

- An inventory log must be kept of equipment issued and to whom it is issued by the Network Manager.
- All documentation must be transported in a sealed bag or file.
- Files and equipment should not normally be left in an unattended vehicle. If it is absolutely necessary to leave something in a vehicle, lock it in the boot. However, if files or equipment contain sensitive (such as case) notes, they must not be left in a vehicle except in an emergency situation.
- When files or equipment are stored at home they should not be openly accessible to other members of the household or visible from outside the premises.
- Password protection should be used wherever possible on mobile equipment.
- Data and confidential information such as student's reports must always be stored in files and encrypted when using laptops and portable hard drives.
- Only USB pens with password facility and encrypted should be used for data storage and confidential information. Where possible it is recommended that staff use Google drive.
- Confidential information should not be discussed in a public area or where it can be overheard by family members. Do not display personal or confidential information on your laptop or on paperwork in a public place.
- Sensitive or confidential information must not be stored on non-school IT equipment. Non-sensitive documents, such as policies or non-sensitive reports may be worked on but deleted after use.
- All thefts/losses of equipment will be reported to the Police and Head teacher.
- When staff leave the employ of the school, all equipment, files and data must be retrieved.

Passwords

- Screensaver passwords must be in use and unattended computers must be switched off, locked or password protected.
- All employees must have their own unique user ID and password and must not share these with any other employee.
- You must not disclose passwords to anyone else, must not write them down, and must not choose obvious passwords.
- You must ensure that passwords are changed regularly. Passwords must consist of at least six characters.
- Employees who suspect that their password has been breached must immediately change it and report the breach to the Head teacher.

Virus Protection

- If a computer virus infection is suspected or detected, the school's ICT support must be contacted immediately.

Security Incidents

- All actual or suspected breaches of security and/or the security policy must be reported to the Head teacher.

If you wish to report a confidential matter, such as misuse of email, this must be reported to the Head teacher (via your line manager if appropriate).

Use of Equipment and Information

- Disposal of computer equipment must be via the school's Network Manager and have Governors' approval.
- Backup files must be stored in secure locations, and in addition, a copy must be removed to a secure off-site location.

Internet

- **Internet usage must comply with the school's Acceptable Use Policy. You are not permitted to access websites containing adult material. Information relating to drugs, gambling, racism, terrorism, violence or weapons may only be accessed for specific work purposes, such as appropriate lesson planning.**

Email

- **Electronic mail must be used in accordance with the Council's Electronic Communication Policy and you are not permitted to circulate emails containing adult material. Information relating to drugs, gambling, racism, terrorism, violence or weapons may not be circulated, unless specifically required for work purposes, such as appropriate lesson planning.**
- The content of electronic mail messages are regarded as a form of publication and are subject to libel laws. Messages must not have any content which could be considered as defamation, harassment or discrimination.
- Individuals have a right of access to information held about them, including information on emails. Ensure that all comments are accurate, justified and professionally worded.
- Email is issued via a unique user ID. You must not allow anyone else to use this user ID.
- You must never attempt to sign on using anyone else's user ID and password.
- Use of internet based email accounts (such as Hotmail) are prohibited.
- Use of the internet and email is recorded and will be monitored.
- School Gmail accounts should only be used for work related purposes.

Training

- Training needs connected to data security will be identified at the SLT ICT review within the school self-evaluation cycle.

Premises Management

Premises management is the responsibility of the Premises Management Team and Network Manager who should ensure:-

- Equipment is sited away from, and protected against, hazards such as water pipes or heaters.
- Suitable fire- fighting equipment is available.
- Buildings are protected by an appropriate intruder detection and alarm system.

Security Incidents

On determining the possibility of a security incident, the Head teacher will assemble a resolution team who will formulate:

- A communications plan, including escalation procedures.
- A Plan of Action for rapid resolution.
- A Plan of Action for non-recurrence.
- A knowledge base of past security incidents, including steps taken for resolution and non-recurrence.

Personal data The first step in processing personal data correctly is recognising it. **Personal data** is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews. **Sensitive personal data** is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

Confidential information refers to anything listed in the blue box above.

All staff need to be aware of how they handle pupil and staff information both electronically and on paper. Staff should have read thoroughly, and signed, the AUP.

Printing

Staff must ensure that when they are printing anything with personal data and sensitive personal data that the documents are collected immediately from the printers. Nothing confidential should be left on the printers and if you find that it has been then it should be disposed of securely in the shredding boxes provided around school **NOT in the recycling bin.**

Paper Files

Staff should be aware of the risks of having confidential paperwork lying about unsecured on desks. These files should either be locked away securely or, if not needed, disposed of in the confidential shredding boxes provided around school. Now that the VPN and staff shares are accessible from home and work please consider whether you need to print documents.

Care Plans & Off-site Documents

Care plans, and any other confidential documents taken off site, need to be kept securely with staff at all times.